## CLAIMS

What is claimed is:

1. A method for providing recipient-end security for transmitted data, the method comprising:

scanning a hard copy document to generate scanned data;

configuring the scanned data so as to require recipient-end security;

transmitting the scanned data to an intended recipient;

determining if the transmitted data may be accessed at the recipient end; and

denying access to the transmitted data if it is determined that the transmitted data may not be accessed.

2. The method of claim 1, wherein scanning a hard copy document comprises scanning a hard copy document using a data transmitting device that transmitted the scanned data to an intended recipient.

3. The method of claim 1, wherein configuring the scanned data comprises configuring the scanned data such that recipient-specific security information must be provided by a recipient of the transmitted data prior to accessing the transmitted data.

4. The method of claim 3, wherein configuring the scanned data comprises configuring the scanned data such that the recipient must provide at least one of a recipient password and recipient biometric information to access the transmitted data.

5. The method of claim 1, wherein configuring the scanned data comprises configuring the scanned data such that machine-specific security data must be verified prior to accessing the transmitted data.

6. The method of claim 5, wherein configuring the scanned data comprises configuring the scanned data such that at least one of a global logon password, an Internet protocol (IP) address, and a media access control (MAC) address of a data receiving device that received the transmitted data is verified.

7. The method of claim 1, wherein transmitting the scanned data comprises faxing the scanned data.

8. The method of claim 1, wherein transmitting the scanned data comprises digitally sending the scanned data as an email attachment.

9. The method of claim 1, wherein determining if the transmitted data may be accessed comprises verifying required recipient-specific security information provided by a recipient that intends to access the transmitted data.

10. The method of claim 9, wherein verifying required recipient-specific security information comprises verifying at least one of a recipient password and recipient biometric information.

11. The method of claim 1, wherein determining if the transmitted data may be accessed comprises verifying required machine-specific security information.

12. The method of claim 11, wherein verifying required machine-specific security information comprises verifying at least one of a global logon password, an Internet protocol (IP) address, and a media access control (MAC) address of a data receiving device that received the transmitted data is verified.

13. The method of claim 1, further comprising providing access to the transmitted data if it is determined that the transmitted data may be accessed at the recipient end.

14. The method of claim 13, wherein providing access comprises at least one of printing out the transmitted data and opening an email attachment that comprises the transmitted data.

15. A system for providing recipient-end security for transmitted data, the system comprising:

means for configuring scanned data representative of a hard copy document so as to require recipient-end security at a recipient end of a transmission path;

means for determining if the scanned data may be accessed at the recipient end by requiring at least one of recipient-specific security information and machine-specific security information; and

means for denying access to the transmitted data if it is determined that the required security information is not correct.

16. The system of claim 15, wherein the means for configuring comprise means for configuring the scanned data such that at least one of a recipient password and recipient biometric information is required to access the scanned data.

17. The system of claim 15, wherein the means for configuring comprise means for configuring the scanned data such that at least one of a global logon password, an Internet protocol (IP) address, and a media access control (MAC) address of a data receiving device that received the transmitted data is required to access the scanned data.

18. The system of claim 15, wherein the means for determining comprise means for verifying at least one of a recipient password and recipient biometric information.

19. The system of claim 15, wherein the means for verifying comprise means for verifying at least one of a global logon password, an Internet protocol (IP) address, and a media access control (MAC) address of a data receiving device that received the transmitted data is verified.

20. A system stored on a computer-readable medium, the system comprising:

sender-end logic adapted to execute on a data transmitting device, the sender-end logic being configured to configure data scanned by the data transmitting device so as to require recipient-end security at a recipient end of a transmission path; and

recipient-end logic adapted to execute on a data receiving device, the recipient-end logic being configured to determine if the scanned data may be accessed at the recipient end by verifying at least one of recipient-specific security information provided by a recipient of the scanned data and machine-specific security information of the data receiving device.

21. The system of claim 20, wherein the sender-end logic is configured to require at least one of a recipient password and recipient biometric information of the recipient prior to access of the scanned data.

22. The system of claim 20, wherein the sender-end logic is configured to require at least one of a global logon password, an Internet protocol (IP) address, and a media access control (MAC) address of a data receiving device that received the transmitted data is verified before a recipient access the scanned data.

23. The system of claim 20, wherein the recipient-end logic is configured to verify at least one of a recipient password and recipient biometric information prior to providing access to the scanned data.

24. The system of claim 20, wherein the recipient-end logic is configured to verify at least one of a global logon password, an Internet protocol (IP) address, and a media access control (MAC) address of a data receiving device that received the transmitted data prior to providing access to the scanned data.

25. A sender-end security manager stored on a computer-readable medium of a data transmitting device, the manager comprising:

logic configured to identify a type of recipient-end security to provide for a data scanned by the data transmitting device; and

logic configured to configure the scanned data to facilitate the identified type of recipient-end security.

26. The manager of claim 25, wherein the logic configured to configure the scanned data comprises logic configured to add security information to the scanned data that is to be used as a reference against recipient-specific security information entered by a recipient of the scanned data.

27. The manager of claim 25, wherein the logic configured to configure the scanned data comprises logic configured to add an executable that is configured to verify at least one of recipient-specific security information entered by a recipient of the scanned data and machine-specific security information of a data receiving device that received the scanned data.

28. The manager of claim 25, wherein the logic configured to configure the scanned data comprises logic configured to add an instruction to the scanned data that indicates to a recipient-end security manager what tasks are to be performed to provided recipient-end security.

29. A recipient-end security manager stored on a computer-readable medium of a data receiving device, the manager comprising:

logic configured to identify a type of recipient-end security that is required to access data that has been received by the data receiving device; and

logic configured to verify recipient-end security information prior to enabling access to the data.

30. The manager of claim 29, wherein the logic configured to verify recipient-end security information comprises logic configured to verify at least one of a recipient password and recipient biometric information.

31. The manager of claim 29, wherein the logic configured to verify recipient-end security information comprises logic configured to verify at least one of a global logon password, an Internet protocol (IP) address, and a media access control (MAC) address of the data receiving device.